AMENDMENTS TO CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method for protecting a ~~security data memory~~ secured data storage (1), ~~wherein~~ by using sensors (2) to detect an external action on a component containing the ~~security data memory~~ secured data storage (1) ~~is detected by sensors (2)~~, comprising the steps of:

determining that an attack ~~being signaled by~~ has occurred based on undershooting or overshooting of a threshold on one of the sensors (2)[[,]];

~~by reason of which the~~ at least partially erasing a content of the ~~security data memory~~ secured data storage (1) ~~is at least partly erased~~[[,]]; ~~characterized in that the~~

permanently monitoring a status of the sensors (2) ~~is permanently monitored~~; and

~~the~~ recording status data of the sensors (2) ~~is recorded~~.

2. (Currently Amended) A method according to claim 1, ~~characterized in that~~ wherein the step of recording said status data comprises the step of storing the status data of the sensors (2) ~~are stored~~ cyclically in an overwritable memory (3).

3. (Currently Amended) A method according to claim 1, ~~characterized in that~~ wherein the step of recording said status data comprises the step of storing the status data of the sensors (2) ~~are stored~~ in a nonvolatile memory (4).

4. (Currently Amended) A method according to claim 1, ~~characterized in that~~ wherein the step of recording said status data comprises the step of storing the status data of the sensors (2) ~~are stored~~ in a volatile temporary memory (3) and when an attack is signaled, transferring the status data contained in the temporary memory (3) ~~are transferred~~ to a nonvolatile final memory (4).

5. (Currently Amended) A method according to claim 4, ~~characterized in that~~ wherein when an attack is signaled at least the status data of the sensor signaling the attack are stored directly in the final memory (4).

6. (Currently Amended) A method according to claim 5, ~~characterized in that~~ wherein the status data are stored in the temporary memory (3) in digitally coded form, and direct storage of the status data in the final memory (4) is done in analog form when an attack is signaled.

7. (Currently Amended) A method according to claim 1, ~~characterized in that~~ further comprising the step of, if the supply voltage (*VCC*) fails, ~~the~~ maintaining a power supply to the sensors (2) and/or the ~~security data memory~~ secured data storage (1), and/or further components (3, 4, 5, 6, 7) required for carrying out the method ~~is maintained~~ with a battery for a certain time period.

8. (Currently Amended) A method according to claim 5, ~~characterized in that~~ wherein after an attack is signaled the content of the ~~security data memory~~ secured data storage (1) is first erased, then the current status data at least of the sensor signaling the attack are stored in the final memory (4), and subsequently the status data contained in the temporary memory (3) are transferred to the final memory (4).

9. (Currently Amended) A method according to claim 1, ~~characterized in that~~ wherein the step of recording said status data comprises the step of transferring the status data stored in the temporary memory (3) ~~are transferred~~ to the final memory (4) in reverse chronological order in terms of their age, the status data of the sensor signaling the attack being transferred first and then the status data of the other sensors.

10. (Currently Amended) A security processor, comprising: ~~having~~

a ~~security data memory~~ secured data storage (1); ~~and~~

sensors (2) for detecting external action on the security processor and/or the ~~security data memory~~ secured data storage (1)[[,]]; ~~and~~

a sensor evaluation device (5) which at least partly erases ~~the~~ a content ~~for~~ of the ~~security data memory~~ secured data storage (1) when a threshold is overshot on one of the sensors (2)[[,]]; and

~~characterized by~~ a data recording device (6) which permanently records the status data of the sensors (2) in a memory (3).

11. (Currently Amended) A security processor according to claim 10, ~~characterized by~~ wherein said memory is an overwritable memory (3) in which the status data of the sensors (2) can be cyclically stored by the data recording device (6).

12. (Currently Amended) A security processor according to claim 10, ~~characterized by~~ wherein said memory includes a volatile temporary memory (3) in which the status data of the sensors (2) are stored permanently, and a nonvolatile final memory (4) to which the status data contained in the temporary memory (3) are transferred when an attack is signaled.

13. (Currently Amended) A security processor according to claim 10, ~~characterized by~~ wherein said memory includes a volatile temporary memory (3) in which the status data of the sensors (2) are stored permanently, and a nonvolatile final memory (4) to which the status data contained in the temporary memory (3) are transferred when an attack is signaled.

14. (Currently Amended) A security processor according to claim 14, ~~characterized by~~ further comprising an analog-to-digital converter (7) which digitally codes the analog status data before storage.

15. (Currently Amended) A security processor according to claim 13, ~~characterized in that~~ wherein the sensor evaluation device (5) is connected with the final memory (4) and when an attack is signaled at least the status data of the sensor signaling the attack are stored directly in the final memory (4).

16. (Currently Amended) A security processor according to claim 1, ~~characterized by~~ further comprising a battery which maintains ~~the~~ a power supply to the sensors (2), and/or ~~security data memory~~ secured data storage (1), and/or sensor evaluation device (5), and/or data recording device (6), and/or data recording device (6) for the status data of the sensors for a certain time period if the supply voltage (*VCC*) fails.

17. (Canceled)

18. (Canceled)